An advantages and disadvantages of Block and Stream Cipher

AUDIA_S_ABD AL_R_ASEDY
Basic Education College
Science Department

AMEER A.J AL_ SWIDI
College of Education
Mathematics Department

Abstract:

In this paper we present a comparison between block and stream ciphers through advantages and disadvantages of both .

1-Introduction:

In1999 the Bluetooth specification was published in the documents describing the new short –range link solutions the researchers presented a stream cipher called E0 which was designed to provide the wireless connection with a strong protection against eavesdroppingE0 .

The E0 encryption system is built around a relatively simple key stream generator which is initialized with a key of at most 128 bit. See [1],[2],[5]

In this research a brief E0 algorithms is presented with two possible improvements are listed.

2-Some Basic Concepts:

the cryptography system divided into crypto analysis (is the science of breaking the cipher) and cryptography is divided into depending on encryption and decryption key and Depending on Cryptographic Techniques :

1-Depending on encryption and Decryption Key :

A-Symmetric Algorithm

C=Ek(M) ,M=DK(C)

K is secret single key ,one key algorithm

i.e. the same key for encryption and decryption

Or the key of decryption .can be calculated from encryption key

B- Asymmetric Algorithm :(public key)Algorithm.

Two key: one for encryption and the second for Decryption.

i.e. C=Ek1 (M) ,M=Dk2(c) ,normally ,k1, is public ,k2 is secret.

2- Depending on Cryptographic Techniques:

I:Block Cipher

Let M be a plaintext message .A block cipher breaks M into successive blocks M1,M2,………,and enciphers for each M1with the same key k,that is EK(M)=EK(M1)EK(M2)…………….

Each block is typically several characters long.

Example(on block cipher):

1-play fair cipher: it is a block cipher of size 2 letters .

2-Hill cipher :it is a block cipher of size d letters.

3-DES cipher: it is a block cipher of size 64 bits .

4-Electronic code Book code book.(ECB)

Corresponding plain text block to a cipher block

Manually: choose 1000-10,000 plain text blocks in a two part book: one for encipherment sorted on plain text the second part sorted on cipher text .

Electronic: each key has different code book, book size is bigger than of manual.

5-transposition with period d character.

6-simple substitution with 1 character.

7-Homophonic substitution with 1 character .

8-Knapsack of length n bits.

II:Stream Cipher

It is breaks the message M into successive characters or bits M1,M2,………,and enciphers each Mi with the it element k_i of a key stream K=K1K2 ……… That is EK(M)=EK1(M1)EK2(M2)

Example(on stream cipher):

1-one time bits and Running key ciphers are non periodic .

2-vigenere cipher is periodic because plain text char are enciphered one –by-one and adjacent char are encipher with a different part of the key.

3-Auto key cipher: An Auto key cipher is example on self-synchronous such that the key is derived from the message it encipher in vigeneres first cipher the key is formed by appending the plain text M=m1m2 ....to a "priming key" character k_i ,the i-th key character (i>1))starts with k1, next key $k_i=m_{i-1}$ or c_{i-1}.

4-cipher feedback (CFB):it is another example on self- synchronous such that plain text is encipher in small units (smaller than block size) .

A stream cipher is periodic if the key stream repeats after characters for some fixed d otherwise it is no periodic.

III: There are two different approaches to stream encryption ,

1- Synchronous stream cipher: key stream is generated independently of the plaintext stream.
2-Self-Synchronous stream cipher: each key character(or bit) is derived from a fixed number n of preceding cipher text character (or bit),For more detail see [3],[4],[6]

IV:Linear Feedback Shift Registers

An n-stage liner Feedback Shift Registers (LFSR) consists of a shift register $R=(r_n,r_{n-1},\ldots.r_1)$ and a ''tap'' Sequence $T=(t_n,t_{n-1}\ldots.,t_1)$, where each r_i and t_i is one binary digit .At each step ,bit r_i is appended to the key stream ,bits $r_n,\ldots.r_2$ are shifted right ,and a new bit derived from T and R is inserted into he left of the register .Letting $R'=(r'_n,r'_{n-1}\ldots r'_1)$ denote the next state of R ,we see that the computation of R' is thus :

$r'_i=r'_{i+1}$ i=1,............,n-1

$r'_n=TR=\ t_i r_i \bmod 2=t_1r_1+t_2r_2+\ldots\ldots\ldots.t_nr_n$

thus R'=HR mod 2, where H is nõn matrix

$$H=\begin{bmatrix} t_n & t_{n-1} & t_{n-2} & & t_3 & t_2 & t_1 \\ 1 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 1 & 0 & & 0 & 0 & 0 \\ . & . & . & & . & . & . \\ 0 & 0 & 0 & & 0 & 1 & 0 \end{bmatrix}$$

An n-stage LFSR can generate pseudo –random bit strings with a period of 2^{n-1}.To achieve this, the tap sequence before repeating .This will happen if the polynomial

$T(x)=t_n x^n + t_{n-1} x^{n-1} + \ldots\ldots + t_1 x + 1$,Formed the form the elements in the tap sequence plus the constant 1,is primitive A primitive polynomial of degree n is an irreducible polynomial that device $x^{2-1}+1$, but not x^d+1 for any that divides 2^n-1primitive trinomials of the form $T(X) = X^n + X^a + 1$are particularly appealing ,because only two stages of the feedback register need be taped see[2],[5].

The polynomial $T(X) = X^4 + X + 1$ is primitive, so the register will cycle through all 15 nonzero bit combination in $GF(2^3)$before repeating . Now as $T(x) = X^4 + X + 1$, tap sequence T=(1,0,0,1),i.e. $x^4=1$,$x^3=0$,$x^2=0$,x=1. the matrix H is given by

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Starting R in the initial state 0001 .we have

0	0	0	1
1	0	0	0
1	1	0	0
1	1	1	0
1	1	1	1
0	1	1	1
1	0	1	1
0	1	0	1
1	0	1	0
1	1	0	1
0	1	1	0
0	0	1	1
1	0	0	1
0	1	0	0
0	0	1	0

The rightmost column gives the key stream k=100011110101100.for more detail

see [2],[3],[4]

3.Previous Attacks on E0:

As is usual in cryptanalysis ,we focus on known –plaintext attacks, i.e.we assume a situation in which the attacker is able to obtain a certain amount of decrypted text in one way or another . The goal of a known –plaintext attack is to use this information to recover other (unknown) parts of the plaintext .In the case of additive stream ciphers, this problem reduces to finding a way to predict the entire key stream zt given a limited number of key stream bits.

To derive the output bits of the key stream generator described in the previous section ,at least two fundamentally different methods:

1:Correlation Attacks.

2: Guess and Determine Attacks.

4.Advantages of block cipher:

1-It is some what faster than stream cipher each time n characters executed.

2-Transmission errors in one cipher text block have no affect on other blocks.

3-Not sufficient in hardware but may be used to connect keyboard to cpu(central process unit) because the keyboard is slowly and the transmission data between keyboard and cpu passed through bandwidth 8-bit or 8-character.

4-Block ciphers can be easier to implement in software ,because the often avoid time-consuming bit manipulations and they operate on data in computer-sized blocks

5-More suitable In trading applications.

6-Short blocks at the end of a message must also be added with blank or zero.

7-In the real world block ciphers seem to be more general (i.e. they can be used in any of the four modes, the modes is ECB, CBC,OFB , CFB).

5. disadvantages of block cipher: :

1-Identical blocks of plaintext produce identical blocks of cipher text .

2-Easy to insert or delete blocks .

3-modifying blocks .

4-Block encryption may be more susceptible to cryptanalysis than either stream mode.

Because identical block of plain text yield identical blocks of cipher text.

5-Block encryption is more susceptible to replay than stream encryption if each block is in dependently encipher while the same key one block can be replayed for another.

6. advantages of stream cipher :.

1-Stream cipher that only encryption and decryption data one bit at a time are really suitable For hard ware implementation .

2-Stream cipher it is lase than susceptible to cryptanalysis than either block mode because identical parts of M are encipher with different parts of the key streams.

3-Stream cipher is lase than to vulnerable to insertion or deletion of block.

4-Easy to analyze mathematically .

5-The key stream is generated independently of the message stream.

6-More suitable in military applications.

7-Synchronous stream cipher protect against cipher text searching because identical block of characters in the message stream are enciphered under a different part of the key stream.

8-In self-synchronous stream cipher each key character is derived from a fixed number n of preceding cipher text characters(or bits).

9-Self-synchronous stream ciphers are non-periodic because each key character is function dependent on the entire preceding message stream.
10-Self – synchronous cipher protect a against cipher text searching

because different parts of the message stream are enciphered under different parts of the key stream.

11-Self – synchronous cipher protect against all type of authenticity threats because any change to the cipher text affects the key stream indeed the last block of cipher text is functionally dependent on the entire message serving as a checksum for the entire message.

7.Disadvantage of stream cipher:.

1-Transmission error in 0ne cipher text block have affect on other block such that if a bit lost or a altered during transmission the error affect the n character and cipher resynchronous it self after n correct cipher text char.

2-It is slower than block but we can make it more fast by implemented in special purpose hardware capable of encryption several million bits for second.

3-If the key short length it is mean repeat faster ,so it is because same block .

4-Not suitable in the software .

5-In synchronous stream cipher if a cipher text character is lost during transmission the sender and receiver must resynchronous their key generators before they can proceed further.

6-In self – synchronous stream if a cipher text character is lost or altered during transmission ,the error propagates forward for n characters. But the cipher resynchronous by itself after n correct cipher text characters have been received.

7-Synchronous stream cipher is periodic because key stream is repeater after d character.

8.Conclusions:

1-The statistical attack cannot be applied to the actual E0 algorithm ,as it assumes sequences of consecutive key stream bits which are considerably longer than the maximum packet size.

2-so that to determine which is better to use the block or stream cipher is depends on the requirement of the particular application we can make some general observation about the efficiency and security of the different approaches.

3-we notice that in Bluetooth method the stream cipher is used because the transmission is wireless and for the security side the connection between two person for sent information(message ,picture and phone number,....etc) i.e. between two mobile or between two pc computer or between pc computer and mobile such that in this method the mobile is work same flash Rom , using method of cryptography (Correlation, Guess methods) for this purpose .

Reference

[1] Bruces. “Applied cryptography”, second edition, published by john Wiley and sons ,inc.1996.

[2] Christophe De Canniere ,Thomas Tohansson and Bart preneel cosic internal report- "Cryptanalysis of the blue tooth stream cipher"2001.

[3] JEAN_PAUL TREMBLAY ,PAUL G.SOR ENSON “AN introduction to data structures with application” by mc Graw_Hill,inc,1984.

[4] Jennifer s. and Josef p.”cryptography:An introduction to com puter security”,1989 by prentice Hall of Astralia pty lid.

[5] Shimada M.”Another practical public key cryptosystem”,Electronics letters,vol. no.23,1992,p.2146-2147.